Security Analysis of CCC Digital Key 4.0



The Car Connectivity Consortium Digital Key specifications define how phones and vehicles establish secure access, combining multiple radio technologies such as NFC, BLE, and UWB. CCC publicly describes UWB in Digital Key as using secure distance bounding with cryptographically secured time of flight measurements. Meanwhile, the research community has shown that practical UWB distance reduction attacks exist against commercial chips, and that receiver implementations and verification thresholds matter significantly. This project targets a focused and high impact question: what are the concrete security properties achieved by the latest CCC Digital Key generation in realistic adversarial settings, and where do security assumptions depend on implementation choices that are not obvious from high level descriptions.

During the internship, the intern will model the CCC Digital Key 4.0 architecture at the protocol level and identify the security critical sub protocols: provisioning and key lifecycle, proximity verification and ranging session establishment, and the binding between ranging results and authorisation decisions such as unlock and start. The intern will then perform a structured security analysis using a combination of formal modelling for the cryptographic handshake and systems analysis for cross layer assumptions. The key aim is to identify downgrade surfaces, confusion between BLE and UWB roles, reliance on device state that may reset, and the extent to which distance bounding results are cryptographically and semantically bound to the authorisation state. If access to implementations or evaluation platforms is available, the intern will validate key parts of the analysis empirically, for example by testing how ranging failures, interference, or partial sessions affect the final unlock decision.

Practicalities

Supervisors:	Sayon Duttagupta	sayon.duttagupta@esat.kuleuven.be	office B01.17
	Nikola Antonijević	nikola.antonijevic@esat.kuleuven.be	office B01.17
	Amit Singh Bhati	amitsingh.bhati@3milabs.tech	office B01.17
	Varesh Mishra	varesh.mishra@esat.kuleuven.be	office B01.23
	Dominik Roy George	dgeorge@esat.kuleuven.be	office B01.24
	Aysajan Abidin	aabidin@esat.kuleuven.be	office 01.13

Nature of the work:	20% literature, 20% theoretical work, 60% software
Number of students:	1

 © 2025-2026 COSIC